6. Popovic D. (2006). Modelling the marketing of high-tech start-ups. Journal of Targeting, Measurement and Analysis for Marketing, 14 (3): 260-276.
7. Schultz D. E. (2001). Marketers: Bid Farewell to Strategy Based on Old 4Ps. Marketing News, 35 (2): 7.
8. Yudelson J. (1999). Adapting McCarthy's Four P's for the Twenty-First Century. Journal of Marketing Education, 21 (1): 60-67.
9. Динамика биржевого показателя NASDAQ Composite Index© https://research.stlouisfed.org/fred2/series/NASDAQCOM#.

РАЗРАБОТКА РЕКОМЕНДАЦИЙ ДЛЯ РЕАЛИЗАЦИИ МЕР ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВЕБ-ИНТЕРФЕЙСОВ ПОЛЬЗОВАТЕЛЕЙ ДЛЯ СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ

О.С. Резниченко,
старший преподаватель кафедры прикладной математики и информационных технологий НИУ «БелГУ»
Н.А. Клименко,
бакалавр 4 года обучения направления подготовки «Бизнес-информатика», НИУ «БелГУ»

В настоящее время все больше увеличивается интерес к решению вопросов информационной безопасности. Развитие информационных технологий и бизнеса в сети Интернет привело к необходимости уделять повышенное внимание защите систем, реализованных с помощью веб-приложений в облаке от действий злоумышленников.

Сетевые ресурсы и сервер, на котором они расположены, связаны с информационной системой организации или могут быть ее частью, и, как правило, непосредственно включены в корпоративную сеть. Существует множество методов несанкционированного использования сетевых ресурсов и проникновения в информационную сеть организации. Вопрос безопасности интерфейса пользователя систем поддержки принятия решений стал актуальным и для всех сфер современного бизнеса, применяющими их.

Реализация интерфейса пользователя любой системы поддержки принятия решений (СППР) веб-средствами требует проведения тщательных мероприятий по защите информации и доступа к данным.

Отсутствие системы защиты СППР может привести к реализации следующих угроз:

1) несанкционированное выполнение команд;
2) загрузка исполняемых кодов и модулей;
3) кража корпоративной и личной информации;
4) модификация контента сетевого сервиса;
5) изменение конфигурации сервера, на котором размещается сетевой сервис.

Источниками проникновения вредоносных скриптов могут являться:

1) Заражение рабочей станции администратора вирусом, перехватывающим FTP пароли и передающим их злоумышленнику или на сервер-распространитель вирусов. Субъектами угроз могут быть пользователи, имеющие доступ на сервер по каналу FTP.

2) Генерация пароля от файлового сервера с помощью специальных утилит для подбора паролей, является типовым методом при целенаправленной хакерской атаке.

3) Использование уязвимостей в скриптах или системах управления контентом – CMS.

4) Применение, внедрение модулей и компонентов, полученных из неизвестных источников, использование скриптов уже содержащих вирусы.

5) Халатность системных администраторов при настройке сервера на хосте.

6) Неопытность владельцев информационного ресурса.

7) Ненадлежащее хранение паролей и их передача по открытым, незащищенным каналам связи.

Основная задача защиты интерфейса пользователя СППР – разработка сетевого ресурса, предельно удовлетворяющего требованиям безопасности путем анализа потенциально опасных уязвимостей с последующим выполнением ряда работ для их устранения.

Безопасность интерфейса пользователя СППР, как и любого сайта складывается из трех аспектов (см. рисунок 1):

- безопасности программной части (CMS и скрипты);
- безопасности сервера;
- безопасность администрирования.

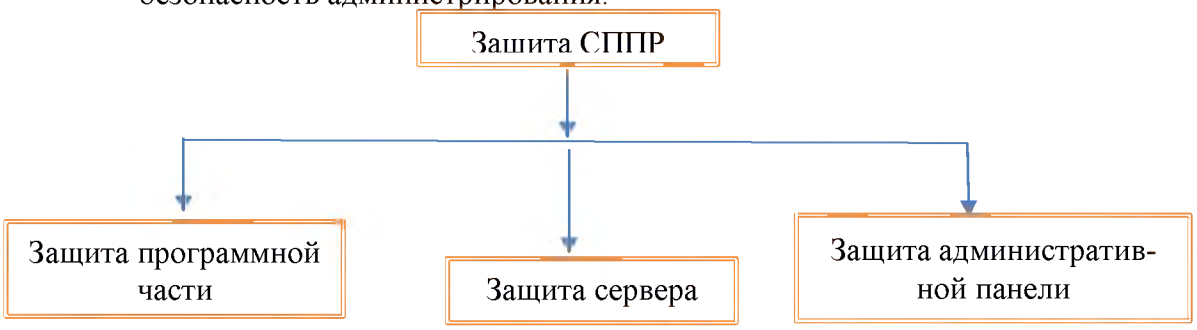

Рис. 1. Компоненты защиты интерфейса пользователя СППР

В зависимости от задач и целей, комплексная защита сетевого ресурса формируется из разных компонентов. Это позволяет найти разумный баланс между уровнем безопасности и денежными затратами.

В программную часть веб-ресурса входят скрипты, на которых основана работа интерфейса пользователя, а также файлы системы управления сайтами (CMS), если таковые применяются в качестве базы для ее реализации.

В ходе анализа мероприятий по защите программной части ресурса были предложены следующие рекомендации:

1) работать по безопасным протоколам SFTP и SCP, рекомендуемая программа в данном случае для работы с файловой системой веб-ресурса— WinSCP;

2) регулярно обновлять скрипты и CMS;

3) периодически сканировать сайт с помощью средств поиска уязвимостей, например, XSpider, Acunetix Web Vulnerability Scanner, утилиты для поиска SQL-инъекций, XSS, RFI и др.;

4) периодически проверять исходный код ресурса средствами статического анализа исходного кода (RIPS);

5) следует подключать веб-ресурс к панелям веб-мастеров поисковых систем (Яндекс, Google и др.);

6) обеспечить правильную настройку конфигурации веб-ресурса, включающую следующие мероприятия:

- права на доступ к файлам и директориям должны быть грамотно прописаны;
- закрыть доступ к файлам конфигурации и каталогам, хранящим резервные копии;
- установка запрета на выполнение скриптов в директориях, предназначенных для загрузки внешних файлов.

7) периодически проводить аудит сайта (с помощью специалистов или программ XSpider 7.5 или Acunetix Web Vulnerability Scanner Enterprise);

8) регулярная проверка сайта детектором вредоносных скриптов (например, «AI-Bolit»).

Вторым не менее важным аспектом по обеспечению безопасности пользовательского интерфейса СППР является сервер, на котором собственно размещается сам веб-ресурс.

Существует два вида предоставления услуги хостинга: общий (shared) и выделенный (dedicated). Отличие между данными видами в ответственности за безопасную настройку сервера, где для shared-хостингов ответственным является администратор хостинг-компании, а для dedicated-сервера (VDS/VPS/DDS) - владелец сервера.

Для реализации интерфейса пользователя СППР наилучшим вариантом является выделенный сервер, при этом в ходе его настройки необходимо придерживаться следующих правил:

1) конфигурация сервера должна обеспечивать минимальную свободу действий при его настройке, так как неопытные пользователи могут нарушить работоспособность веб-ресурса;

2) в случае, если подключение к другим серверам не является необходимым для реализации интерфейса СППР, внешние соединения должны быть закрыты;

3) неиспользуемые функции должны быть отключены;

4) область видимости файловой системы, содержащей исполняемые скрипты, должна быть ограничена и организованы механизмы контроля ее целостности;

5) должна быть обеспечена организация системы резервного копирования и логирования административных действий;

6) выбирать хостинги, предоставляющие персональную настройку сервера.

Панель администратора является командным центром веб-ресурса, через нее можно получить доступ практически ко всем файлам и данным, поэтому получение доступа в административную панель является приоритетной целью злоумышленников.

Были выделены следующие мероприятия по защите административной панели:

1) хранение паролей в надежном месте (применение специальных программ, например, KeePass);

2) регулярная смена паролей, при этом пароли должны состоять из разных комбинаций символов, цифр и знаков;

3) регулярная проверка на вирусы рабочего ПК, с которого происходит администрирование веб-ресурса;

4) закрытие доступа к административной панели по IP;

5) применение двойной авторизации (дополнительная авторизация средствами веб-сервера);

6) применение кодового слова (фразы) при открытии административной панели веб-сервера (разрешение доступа к каталогу на основе фрагмента, который содержится в поле «User Agent» браузера);

7) использование удобных для восприятия веб-адресов (SEF-компонентов);

8) скрытие использования систем управления контентом посредством удаления метатегов;

9) удаление не используемых модулей, компонентов, плагинов, скриптов;

10) замена префиксов в базах данных;

11) использование конфигурационного файла «.htaccess», который необходим для защиты информации о настройках веб-сервера.

Таким образом, чтобы обеспечить защиту пользовательского интерфейса СППР, реализованного в веб-среде, от вредоносных скриптов и деятельности злоумышленников, необходимо уделить достаточное количество времени и ресурсов проблеме безопасности.

Выполнение описанных выше мероприятий поспособствует решению основных задач защиты веб-ресурса. При этом нужно одновременно уделять достаточно внимания трем аспектам его защиты: поддержке ПО в актуальном состоянии, правильному подходу к вопросу настройки хостинга и слежки за правами доступа к веб-ресурсу и защите административной панели. Если хотя бы один из трех элементов будет слабым звеном, веб-интерфейс останется уязвимым.

Исследование выполнено за счет гранта Российского научного фонда, проект №14-38-00047«Прогнозирование и управление социальными рисками развития техногенных человекомерных систем в динамике процессов трансформации среды обитания человека».

Литература

1 Информатика в экономике: Учебное пособие [Текст]/ред. проф. Б.Е. Одинцова, проф. А.Н. Романова. - М.: Вузовский учебник, 2008. - 478 с.

2 Куянцева, Л.М. Информационное общество [Электронный ресурс] / Л.М. Куянцева. - Режим доступа: http://infdeyatchel.narod.ru/inf_ob.htm, свободный. – (дата обращения: 01.04.2014)

3 Шевнина, Ю.С. Разработка в информационной системе интерфейса пользователя, адаптированного к онтологической модели предметной области [Текст] / И.Г. Игнатова, Ю.С. Шевнина, А.Ю. Павлов // Научные исследования и их практическое применение. Современное состояние и пути развития: сб. науч. тр. / Черноморье. – Одесса, 2005. – Том 7: Технические науки. – С. 77–80.

4 Google Analytics. Средства веб-аналитики корпоративного уровня [Электронный ресурс]. – Режим доступа: http://www.google.com/analytics/, свободный. – (дата обращения 01.04.2014).

5 AWStats official web site [Электронный ресурс]. – Режим доступа: http://awstats.sourceforge.net/ свободный. – (дата обращения 01.04.2014)

ДИАПАЗОН РЕПРЕЗЕНТАТИВНОСТИ ДИСТАНЦИОННОГО ЭМПИРИЧЕСКОГО ИССЛЕДОВАНИЯ (ПО МАТЕРИАЛАМ МЕТАПРОЕКТА «ГРАЖДАНСКАЯ ЭКСПЕРТИЗА СФЕРЫ УПРАВЛЕНИЯ»)

А.В. Тихонов,
доктор социологических наук, профессор,
руководитель Центра социологии управления и социальных технологий ИС РАН
В.С. Богданов,
кандидат социологических наук,
старший научный сотрудник Центра социологии управления и социальных технологий ИС РАН

В 2011 году (по н/в) стартовал метапроект ИС РАН «Гражданская экспертиза сферы управления», в рамках которого в экспериментальном порядке была осуществлена интеграция оффлайн и онлайн опросов во всероссийском масштабе с целью проверки возможности получения репрезентативных данных о проблемной ситуации в системе управления страной – от низового до высшего уровня, т.е. по всей властно-управленческой вертикали с помощью дистанционных интернет-технологий.

Целесообразность сочетания двух типов сбора первичных данных была обусловлена ещё и тем, что на момент запуска исследовательского проекта было зафиксировано примерно равно долевое распределение российского населения, как потенциальной генеральной совокупности, по критерию доступа к интернету: 51% - имели такой доступ, и 49% не имели**. Это была** уникальная возможность уже на этапе полевого опроса разделить массив на два подмассива и сравнить ответы пользователей и непользователей интернета по всему предметному полю решаемых проблем, а затем сравнить ответы, полученные дистанционным способом (онлайн) и при помощи полевого опроса (оффлайн). Также следует отметить, что результаты нашего эксперимента корреспондируются с методологическими вопросами, которые ставит И.Ф. Девятко в контексте рассмотрения проблем репрезентативности и валидности данных, получаемых при помощи Интернет, что